BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

E5-00025-TH (1)

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 778 291**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **98 05483**

(51) Int Cl⁶ : **H 04 L 9/32**, H 04 L 9/14, 9/20, G 06 F 1/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 30.04.98.

(30) Priorité :

(43) Date de mise à la disposition du public de la demande : 05.11.99 Bulletin 99/44.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *SCHLUMBERGER INDUSTRIES SA Société anonyme* — FR.

(72) Inventeur(s) : LION STEPHANIE et SION JEROME.

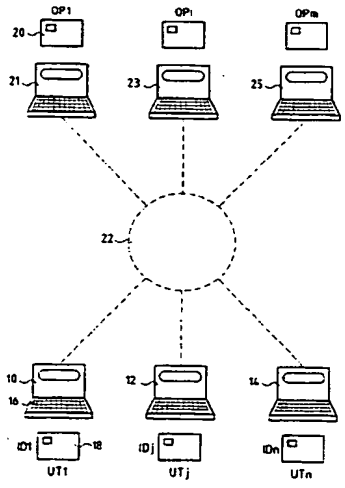
(73) Titulaire(s) :

(74) Mandataire(s) : CABINET BEAU DE LOMENIE.

(54) SYSTEME DE TRANSMISSION PROTEGE D'INFORMATIONS.

(57) L'invention concerne un système de transmission protégé d'informations entre des utilisateurs unis de terminaux (10, 12, 14) et de cartes électroniques (18) et des opérateurs munis également de terminaux (20, 22, 24) et de cartes électroniques (20).

La protection de l'échange d'informations entre utilisateur et opérateur est assurée par la mise en oeuvre chez l'utilisateur et l'opérateur, d'algorithmes à clé non publique. Elle permet la protection vis à vis de l'opérateur et vis à vis de l'utilisateur. Chaque carte d'utilisateur contient en mémoire une information secrète associée à une information d'identification de la carte IDJ.



FR 2 778 291 - A1

La présente invention a pour objet un système de transmission protégé d'informations entre au moins un utilisateur et au moins un opérateur.

De façon plus précise, l'invention concerne un système qui permet, en utilisant une installation de transmission d'informations entre un ou plusieurs utilisateurs et un ou plusieurs opérateurs, de protéger ou sécuriser la transmission de ces informations afin d'éviter toute utilisation frauduleuse du système.

Ce système est du type dans lequel le ou les utilisateurs et le ou les opérateurs doivent disposer d'un support amovible d'informations protégées pour effectuer la transmission de ces informations.

Dans le présent texte, par "support amovible d'informations protégées" il faut entendre un objet amovible équipé de circuits électroniques de mémorisation et de traitement d'informations qui est capable de dialoguer avec un dispositif de lecture/écriture et dans lequel les informations mémorisées sont protégées contre des tentatives d'effractions. Un mode préféré de réalisation d'un tel support est constitué par une carte à microprocesseur.

Il existe aujourd'hui deux grands types de protection de transmission d'informations, ceux qui utilisent un système de cryptage à clé publique et ceux qui utilisent un système de cryptage à clé secrète.

Avec le premier système, une première étape permet d'authentifier l'interlocuteur par la connaissance du couple clé publique/clé secrète et par la certification de l'association clé publique identité de l'utilisateur par une personne de confiance telle que l'opérateur. Une fois établie l'identité de l'émetteur et/ou du récepteur, une clé de cession est élaborée et échangée, cette clé étant utilisée par la suite pour garantir l'intégrité et la confidentialité des échanges. Ces systèmes nécessitent une autorité de confiance et une gestion de certificat. Ils sont le plus souvent réservés à des systèmes dans lesquels il intervient un nombre important et variable d'utilisateurs et aux communications entre utilisateurs.

Dans le deuxième type de système de cryptage, l'opérateur et l'utilisateur partagent une valeur secrète. Cette valeur est utilisée par la suite par l'utilisateur et respectivement l'opérateur pour authentifier l'opérateur respectivement l'utilisateur. L'opérateur dispose d'une base de données qui regroupe la liste de ses utilisateurs et leur clé.

D'autre part, dans la majorité des systèmes hiérarchiques opérateur/utilisateur, c'est l'opérateur qui est à l'initiative des échanges et c'est lui qui contrôle la génération de la clé de cession.

Un objet de la présente invention est de fournir un système de transmission protégée d'informations qui, tout en assurant un haut degré de protection des informations transmises, évite d'une part la mise en oeuvre d'algorithmes du type à clé publique qui sont des algorithmes lourds en calcul, en code et longueur de clé à stocker et d'autre part qui évite d'avoir dans l'installation du côté de l'opérateur une base de données regroupant la liste de ses utilisateurs et leurs clés correspondantes.

Pour atteindre ce but, selon l'invention, le système d'échange d'informations entre au moins un utilisateur et au moins un opérateur se caractérise en ce qu'il comprend :

- au moins un support amovible d'informations protégées utilisateur, chaque support utilisateur étant associé à une information d'identification ID,
- au moins un dispositif de lecture/écriture utilisateur pour recevoir un support utilisateur ;
- au moins support amovible d'informations protégées opérateur ;
- au moins un dispositif de lecture/écriture opérateur pour recevoir un support opérateur ; et
- des moyens de transmission d'informations entre lesdits dispositifs de lecture/écriture ;
- chaque support abonné comprenant :
  . des moyens pour mémoriser une information secrète (UID) résultant de l'application d'un premier algorithme de cryptage (Algo0p1) à ladite information d'identification (ID) avec une première clé secrète (Ks-Op),
  . des moyens pour élaborer des nombres pseudo-aléatoires (R),
  . des moyens de mise en oeuvre d'une première fonction de cryptage utilisant comme clé ladite information secrète (UID), ladite première fonction étant appliquée audit nombre pseudo-aléatoire R ; et
  . des moyens de mise en oeuvre d'une deuxième fonction de cryptage utilisant ledit nombre pseudo-aléatoire (R) comme clé pour appliquer ladite deuxième fonction à une information (Req, réponse),
- chaque support opérateur comprenant :

. des moyens pour mémoriser ladite première clé secrète (Ks-Op).

. des moyens de mise en oeuvre dudit premier algorithme de cryptage (AlgoOp1) utilisant ladite première clé secrète,

. des moyens de mise en oeuvre d'une troisième fonction de cryptage inverse de ladite première fonction de cryptage ; et

. des moyens de mise en oeuvre d'une quatrième fonction de cryptage inverse de ladite deuxième fonction de cryptage ; et

- chaque dispositif de lecture/écriture étant apte à transmettre vers un autre dispositif de lecture/écriture les informations élaborées par le support qu'il contient et à appliquer au support qui y est inséré des informations reçues d'un autre dispositif de lecture/écriture.

On comprend que, pour la mise en oeuvre de ce système, l'opérateur ou chaque opérateur détient un support, par exemple une carte, dans lequel est stockée en mémoire une première clé secrète et que chaque utilisateur détient un support, par exemple une carte, dans lequel est stockée une information secrète associée à son information d'identification. Ces informations étant contenues dans le circuit intégré du support, elles sont très efficacement protégées. On voit également que dans ce système les algorithmes peuvent être beaucoup plus simples que les algorithmes du type à clé publique.

Selon un premier mode de mise en oeuvre, dans le support abonné, le nombre pseudo-aléatoire est obtenu par la mise en oeuvre d'un logiciel de génération de nombres pseudo-aléatoires. Dans ce cas, on comprend que le support abonné ne comprend comme donnée secrète que l'information secrète (UID) mais doit pouvoir mémoriser le nombre pseudo-aléatoire.

Dans un deuxième mode de mise en oeuvre pour l'élaboration du nombre pseudo-aléatoire, le support comprend des moyens de mémorisation d'une deuxième clé secrète, des moyens pour recevoir du dispositif de lecture/écriture utilisateur une information spécifique choisie par l'utilisateur et des moyens de mise en oeuvre d'un deuxième algorithme de cryptage pour appliquer à ladite information spécifique ledit deuxième algorithme de cryptage en utilisant ladite deuxième clé secrète.

Dans ce deuxième mode de mise en oeuvre, le support utilisateur doit comprendre une clé secrète, mais, en raison de l'utilisation de l'information spécifique par l'utilisateur détenteur du support abonné, on peut s'assurer

que c'est bien le même utilisateur qui a émis vers l'opérateur une question et qui ultérieurement va recevoir de l'opérateur la réponse à sa question.

D'autres caractéristiques et avantages de l'invention apparaîtront mieux à la lecture de la description qui suit de plusieurs modes de mise en oeuvre de l'invention donnés à titre d'exemples non limitatifs. La description se réfère aux figures annexées sur lesquelles :

- la figure 1 est un schéma simplifié de l'installation d'échange d'informations ;
- la figure 2 est un exemple de réalisation simplifié des circuits présents dans les cartes opérateur ou utilisateur ;
- la figure 3 est un organigramme montrant les différentes opérations pour l'émission d'un message par l'utilisateur vers l'opérateur ;
- la figure 4 montre d'une part un organigramme correspondant aux opérations de réception d'un message émis par l'utilisateur et reçu par l'opérateur et d'autre part les opérations correspondant à l'émission par l'opérateur vers un utilisateur d'un message de réponse ; et
- la figure 5 est un organigramme montrant les opérations de réception par l'utilisateur d'un message émis par l'opérateur.

En se référant tout d'abord à la figure 1, on va décrire un exemple d'installation permettant la mise en oeuvre du système utilisant des cartes à microprocesseur. On trouve d'une part un certain nombre de terminaux utilisateurs 10, 12... 14 qui consistent essentiellement dans des dispositifs de lecture/écriture de carte à microprocesseur comportant des moyens, par exemple un clavier, pour l'introduction d'informations, ces claviers étant référencés de manière générique 16. Chaque utilisateur UT1, UTJ, UTn est équipé d'une carte à mémoire électronique 18, chaque utilisateur détenant une information d'identification ID1, Idj, Idn. On trouve également des terminaux opérateurs 21, 23 ... 25 qui ont exactement la même organiquement que les terminaux utilisateurs. Chaque opérateur détient une carte à mémoire électronique 20, les opérateurs étant repérés par OP1, OPi, OP_m. Un système d'intercommunication 22 permet de façon parfaitement connue de relier en réseau les différents terminaux utilisateurs aux différents terminaux opérateurs.

Dans la description qui suit, on envisagera le cas de la transmission d'informations entre un unique utilisateur et un unique opérateur. On

comprend cependant aisément que le système peut, par des moyens connus, être généralisé à plusieurs utilisateurs et plusieurs opérateurs.

Sur la figure 2, on a représenté très schématiquement la structure bien connue des principaux circuits contenus dans la carte à mémoire électronique. On trouve un microprocesseur 24 qui est relié aux plages externes de contact électrique 26 de la carte à mémoire par quoi le microprocesseur peut recevoir des informations elles-mêmes reçues par le dispositif de lecture/écriture ou émettre des informations vers le dispositif de lecture/écriture. Les circuits de la carte comprennent également une mémoire de travail 28 du type RAM, une mémoire programmable 30 pour le stockage des sous-programmes associés aux différents algorithmes ou fonctions de cryptage qui seront mis en oeuvre et une mémoire permanente 32 pour le stockage de données qui seront explicitées ultérieurement.

Si l'on considère tout d'abord une carte abonnée, elle comporte dans ses mémoires les informations suivantes :

un premier sous-programme correspondant à un deuxième algorithme de cryptage AlgoAb1 ; un sous-programme correspondant à un autre algorithme de cryptage AlgoAbo2 qui peut se décomposer en une première fonction de cryptage cryp1 et une deuxième fonction de cryptage crypt 2. Enfin, on trouve un sous-programme correspondant à un troisième algorithme de cryptage consistant dans la fonction de codage crypt 2.

Dans la mémoire de données, on trouve une information scrète UID qui résulte, comme on l'expliquera ultérieurement, de la mise en oeuvre d'un premier algorithme de codage appliqué à l'information d'identification ID. Cette mémoire de donnée comporte également une clé secrète KS/Abo.

Si l'on considère maintenant les informations stockées en mémoire dans une carte opérateur, elles comprennent un premier sous-programme pour la mise en oeuvre d'un premier algorithme de cryptage AlgoOp1 qui est l'algorithme qui permet de passer de l'information d'identification ID à l'information secrète UID en utilisant une première clé secrète Ks-Op qui est mémorisée dans la mémoire de données de la carte opérateur. Dans la mémoire de programme, on trouve également un sous-programme correspondant à la mise en oeuvre d'un quatrième algorithme de cryptage qui consiste en une première fonction de codage décrypt 1 et une deuxième fonction de codage décrypt 2. Les fonctions de codage décrypt 1 et décrypt 2 sont les fonctions inverses des fonctions de codage crypt 1 et crypt 2.

A partir de ces différents éléments, on va expliquer les différentes opérations qui sont mises en oeuvre lorsqu'un utilisateur transmet vers l'opérateur des messages, par exemple pour poser une question, et qu'à la réception de ces messages l'opérateur transmet à son tour d'autres messages consistant par exemple dans la réponse à la question codée.

En se référant maintenant à la figure 3, on va décrire les différentes opérations effectuées par un utilisateur et par les circuits de sa carte pour émettre un message consistant par exemple dans une requête.

L'utilisateur entre dans le lecteur 10 un mot de passe (password) qui le choisit librement. A la réception de ce mot de passe, le micro-processeur de la carte utilisateur met en oeuvre le deuxième algorithme de cryptage AlgoAbo1 en utilisant comme clé de cryptage la clé secrète Ks Abo stockée dans la mémoire de données. On obtient ainsi un nombre pseudo-aléatoire R. L'utilisateur entre alors, à l'aide du dispositif de lecture/écriture, la requête, c'est-à-dire la question qu'il souhaite poser à l'opérateur. En réponse à cette opération, le micro-processeur de la carte utilisateur met en oeuvre le quatrième algorithme de cryptage AlgoAbo2. Dans un premier temps, on met en oeuvre la fonction de codage crypt 1 en utilisant l'information secrète UID comme clé pour coder le nombre pseudo-aléatoire R. On obtient ainsi une première information codée Mess 1. Puis, par mise en oeuvre de la fonction de code crypt 2 appliquée à la requête, en utilisant comme clé le nombre pseudo-aléatoire R, on élabore une deuxième information Mess 2 qui est donc la forme cryptée de la requête. Les informations Mess 1 et Mess 2 ainsi que l'information d'identification ID sont alors émises par le dispositif de lecture/écriture 10 vers le terminal de l'opérateur.

En se référant maintenant à la figure 4, on va décrire les opérations qui interviennent lorsque le terminal d'un opérateur reçoit les informations définies précédemment. Dans une première phase, les informations reçues sont traitées pour en extraire la requête. Cela correspond à la demi-figure de gauche A. Dans un premier temps, l'information d'identification ID est traitée par l'algorithme AlgoOp1 pour obtenir, à partir de ID, l'information secrète UID. Puis, un troisième algorithme de cryptage AlgoOp2 est mis en oeuvre. Plus précisément, dans un premier temps, la fonction de codage décrypt 1 est appliquée à l'information Mess 1 en utilisant comme clé UID. On obtient alors la clé de cession K dont on comprend qu'en fonctionnement

normal elle est identique au nombre aléatoire R. Puis, en utilisant comme clé le nombre K, on met en oeuvre la fonction de codage décrypt 2 appliquée à l'information Mess 2, ce qui permet d'obtenir en clair la requête émise par l'utilisateur. Au vu de cette requête, l'opérateur élabore une réponse à cette requête. Dans un premier temps, l'algorithme de cryptage AlgoOp1, en utilisant la clé secrète de l'opérateur Ks-Op, est appliqué à ID pour retrouver la valeur KID. On comprend que, dans un mode simplifié de réalisation, l'information UID aurait pu être mémorisée temporairement dans la carte opérateur, ce qui permet d'éviter la mise en oeuvre de l'algorithme. En utilisant l'information secrète UID comme clé la fonction de codage décrypt 1 est appliquée à l'information Mess 1, ce qui permet de retrouver le nombre K. Dans une version simplifiée, on pourrait prévoir également de mémoriser dans la carte opérateur la valeur K élaborée précédemment. Puis la fonction de codage décrypt 2 est appliquée à la réponse que l'opérateur a introduite dans la carte. On obtient alors un message crypté Mess 3 qui correspond à la réponse cryptée qui est transmise alors vers le dispositif de lecture/écriture de l'utilisateur qui a émis la question.

En se référant maintenant à la figure 5, on va décrire les opérations qui permettent à l'utilisateur d'obtenir en clair la réponse à sa requête.

L'utilisateur introduit son mot de passe. L'algorithme de cryptage AlgoAbo1 est alors mis en oeuvre en utilisant Ks Abo comme clé de cryptage. On retrouve alors le nombre pseudo-aléatoire R. Dans un deuxième temps, on met en oeuvre un algorithme de cryptage AlgoAbo3 qui consiste dans la fonction de codage crypt 2. Cette fonction de codage est appliquée à l'information Mess 3 pour obtenir en clair la réponse.

Dans un mode de mise en oeuvre simplifié, il est possible d'éviter la mise en oeuvre de l'algorithme de cryptage AlgoAbo1. Dans ce cas, cet algorithme de cryptage est remplacé par un logiciel de génération de nombre pseudo-aléatoire R. On comprend que, dans ce cas corollairement, il n'est pas nécessaire de prévoir une clé secrète Ks Abo dans la carte utilisateur. Cependant, cette simplification qui entraîne la non-utilisation du mot de passe ne permet pas de s'assurer que l'utilisateur qui obtient la réponse est effectivement celui qui y avait droit, c'est-à-dire celui qui avait émis la question.

Comme on l'a indiqué précédemment, au lieu d'utiliser des cartes à microprocesseur comme support amovible d'informations protégées, on pourrait utiliser d'autres objets amovibles équipés de circuits électroniques pour mémoriser des informations et pour traiter celles-ci à condition que les informations soient protégées des effractions comme c'est le cas dans une carte à microprocesseur. Il va également de soi que le dialogue entre le support et le dispositif de lecture/écriture pourrait être réalisé par des signaux autres que des courants électriques comme dans le cas des cartes. On pourrait utiliser une transmission optique, électromagnétique, etc.

REVENDICATIONS

1. Système d'échange d'informations entre au moins un utilisateur et au moins un opérateur, caractérisé en ce qu'il comprend :

- au moins un support amovible d'informations protégées utilisateur, chaque support utilisateur étant associé à une information d'identification ID,
- au moins un dispositif de lecture/écriture utilisateur pour recevoir un support utilisateur ;
- au moins un support amovible d'informations protégées opérateur ;
- au moins un dispositif de lecture/écriture opérateur pour recevoir un support opérateur ; et
- des moyens de transmission d'informations entre lesdits dispositifs de lecture/écriture ;
- chaque support abonné comprenant :
  - . des moyens pour mémoriser une information secrète (UID) résultant de l'application d'un premier algorithme de cryptage (Algo0p1) à ladite information d'identification (ID) avec une première clé secrète (Ks-Op),
  - . des moyens pour élaborer des nombres pseudo-aléatoires (R),
  - . des moyens de mise en oeuvre d'une première fonction de cryptage utilisant comme clé ladite information secrète (UID), ladite première fonction étant appliquée audit nombre pseudo-aléatoire (R) ; et
  - . des moyens de mise en oeuvre d'une deuxième fonction de cryptage utilisant ledit nombre pseudo-aléatoire (R) comme clé pour appliquer ladite deuxième fonction à une information (Req, réponse),
- chaque support opérateur comprenant :
  - . des moyens pour mémoriser ladite première clé secrète (Ks-Op).
  - . des moyens de mise en oeuvre dudit premier algorithme de cryptage (AlgoOp1) utilisant ladite première clé secrète,
  - . des moyens de mise en oeuvre d'une troisième fonction de cryptage inverse de ladite première fonction de cryptage ; et
  - . des moyens de mise en oeuvre d'une quatrième fonction de cryptage inverse de ladite deuxième fonction de cryptage ; et
- chaque dispositif de lecture/écriture étant apte à transmettre vers un autre dispositif de lecture/écriture les informations élaborées par le support

qu'il contient et à appliquer au support qui y est inséré des informations reçues d'un autre dispositif de lecture/écriture.

2. Système d'échange d'informations selon la revendication 1, caractérisé en ce que, pour permettre à un utilisateur de transmettre une première information (Req), ledit support utilisateur comprend en outre :

. des moyens pour recevoir dudit dispositif de lecture/écriture utilisateur ladite première information à transmettre (Req) ;

. des moyens pour commander la mise en oeuvre de ladite première fonction de cryptage, par quoi on obtient un premier message (Mess 1), et pour commander la mise en oeuvre de ladite deuxième fonction de cryptage appliquée à ladite première information à transmettre (Req), par quoi on obtient un deuxième message (Mess 2) ; et

- des moyens pour transmettre audit dispositif de lecture/écriture utilisateur, ladite information d'identification (ID) et lesdits premier (Mess 1) et deuxième (Mess 2) messages.

3. Système d'échange d'informations selon la revendication 2, caractérisé en ce que chaque support opérateur comprend :

- des moyens pour, à la réception desdits premier (Mess 1) et deuxième (Mess 2) messages et de l'information d'identification (ID) :

. appliquer à ladite information d'identification (ID) ledit premier algorithme de cryptage par quoi on obtient ladite information secrète d'identification (UID),

. appliquer audit premier message (Mess 1) ladite troisième fonction de cryptage en utilisant comme clé ladite information secrète d'identification (UID) par quoi on obtient une information de cryptage (K) ; et

. appliquer audit deuxième message (Mess 2) ladite quatrième fonction de cryptage en utilisant ladite information de cryptage (K), par quoi on obtient, dans des conditions normales, ladite première information à transmettre (Req) ; et

- des moyens pour, en réponse à la réception d'une deuxième information à transmettre (Réponse) reçue dudit dispositif de lecture/écriture opérateur :

. commander l'application de ladite quatrième fonction de cryptage à ladite deuxième information à transmettre (Réponse) en utilisant

comme clé ladite information de cryptage (K) par quoi on obtient un troisième message (Mess 3) ; et

. transmettre audit dispositif de lecture/écriture opérateur ledit troisième message (Mess 3).

4. Système selon la revendication 3, caractérisé en ce que ledit support opérateur comprend en outre des moyens pour, en réponse à la réception d'une deuxième information à transmettre (Réponse) reçue dudit dispositif de lecture/écriture opérateur :

. commander la mise en oeuvre dudit premier algorithme de cryptage par quoi on obtient ladite information secrète d'identification (UID),

. commander l'application de ladite troisième fonction de cryptage audit premier message (Mess 1), par quoi on obtient ladite information de cryptage (K) , qui est identique audit nombre pseudo-aléatoire (R) en utilisation normale.

5. Système d'échange d'informations selon la revendication 4, caractérisé en ce qu'il comprend en outre :

- des moyens pour mémoriser ladite information secrète d'identification (UID) obtenue par la mise en oeuvre du premier algorithme de cryptage ; et

- des moyens pour mémoriser ladite information de cryptage (K) obtenue par la mise en oeuvre de ladite troisième fonction de cryptage.

6. Système d'échange d'informations selon l'une quelconque des revendications 1 à 3, caractérisé en ce que lesdits moyens d'élaboration de nombres pseudo-aléatoires du support utilisateur comprennent :

. des moyens de mémorisation d'une deuxième clé secrète (Ks, Abo)

. des moyens pour recevoir dudit dispositif de lecture/écriture utilisateur une information spécifique (password) choisie par l'utilisateur ; et

. des moyens de mise en oeuvre d'un deuxième algorithme de cryptage (AlgoAbo1) pour appliquer à ladite information spécifique ledit deuxième algorithme de cryptage en utilisant ladite deuxième clé secrète.

7. Système de transmission d'informations selon la revendication 6, caractérisé en ce que ledit support utilisateur comprend en outre des moyens pour, à la réception dudit troisième message :

. recevoir dudit dispositif de lecture/écriture utilisateur ladite information spécifique (password),

. appliquer à ladite information spécifique ledit deuxième algorithme de cryptage par quoi on obtient ledit nombre pseudo-aléatoire (R) ; et

. appliquer audit troisième message ladite deuxième fonction de cryptage en utilisant comme clé ledit nombre pseudo-aléatoire, par quoi on obtient ladite deuxième information transmise (Réponse).

8. Système selon l'une quelconque des revendications 1 à 5, caractérisé en ce que ledit support utilisateur comprend en outre :

- des moyens pour mémoriser ledit nombre pseudo-aléatoire (R) ; et
- des moyens pour, à la réception dudit troisième message (Mess 3), appliquer audit troisième message ladite deuxième fonction de cryptage en utilisant comme clé ledit nombre pseudo-aléatoire, par quoi on obtient ladite deuxième information transmise (Réponse).

9. Système selon l'une quelconque des revendications 1 à 8, caractérisé en ce que lesdits supports amovibles d'informations protégées sont des cartes à microprocesseur.

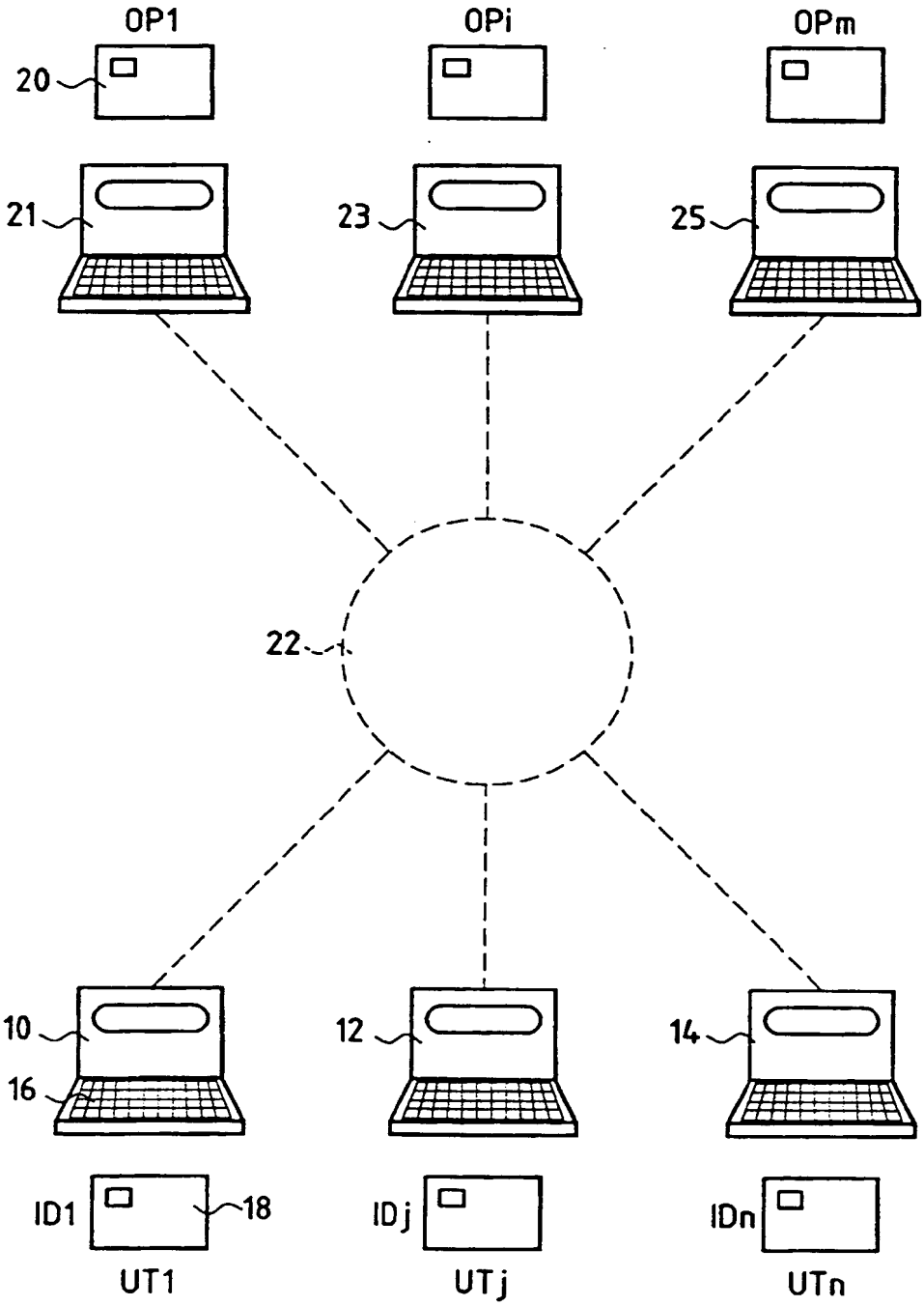


FIG.1

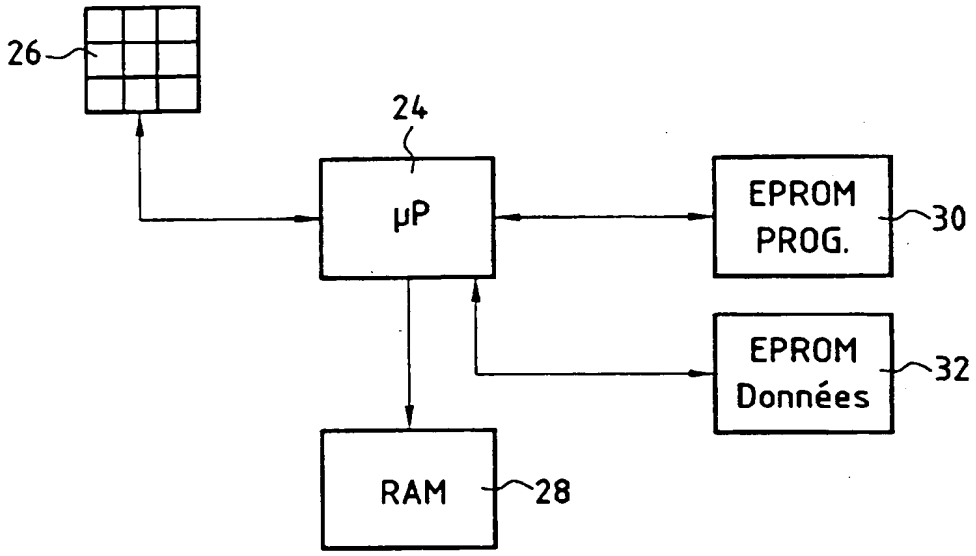


FIG.2

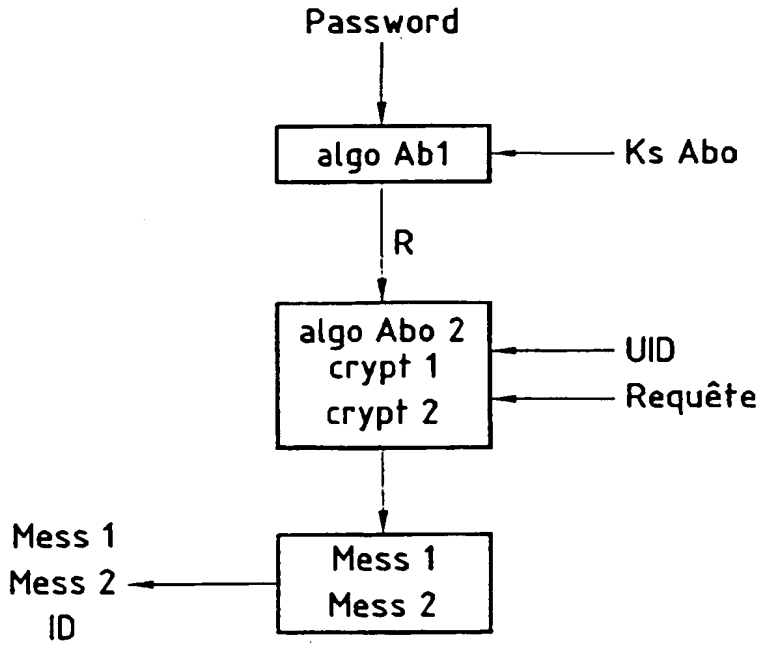


FIG.3

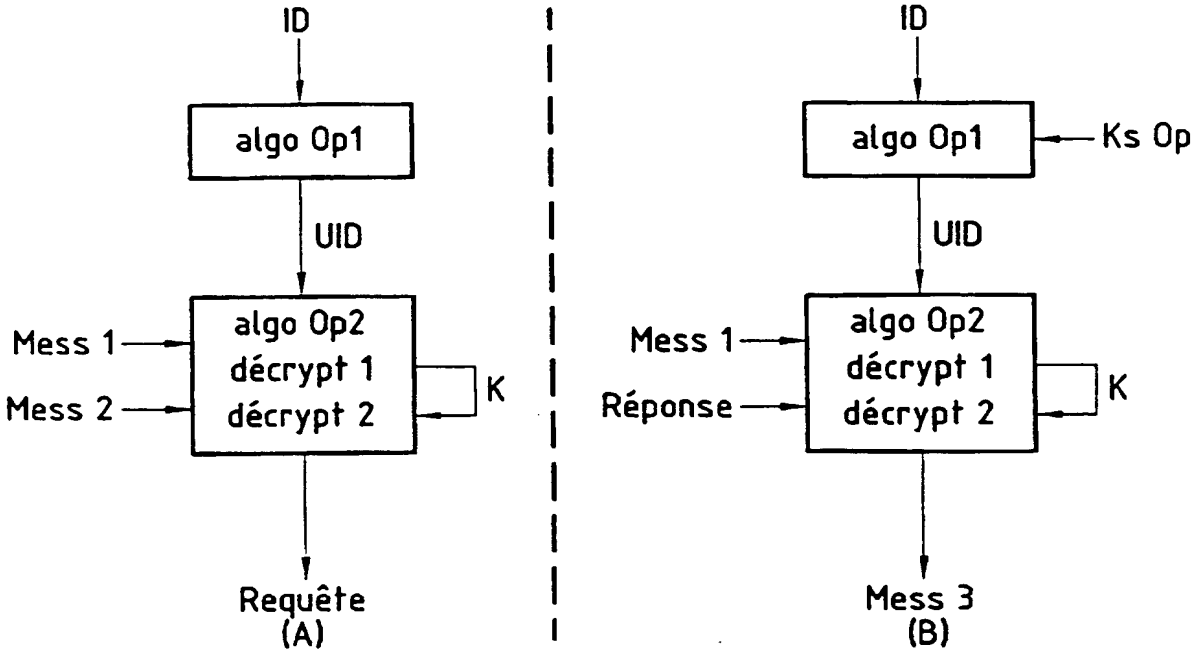


FIG.4

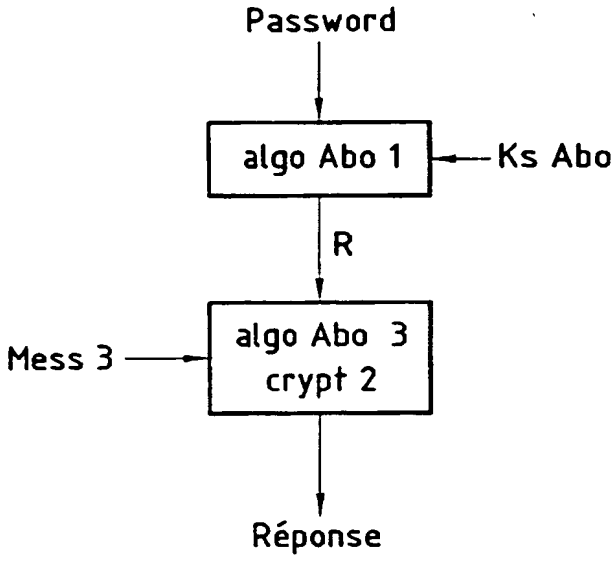


FIG.5

2778291

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 560947
FR 9805483

DOCUMENTS CONSIDERES COMME PERTINENTS

Categorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	EP 0 422 230 A (MATSUSHITA ELECTRIC IND CO LTD) 17 avril 1991 * page 4, ligne 18 - ligne 23 * * page 4, dernier alinéa * * page 5, dernier alinéa - ligne 58 * * page 7, ligne 10 - ligne 54 * * page 12, ligne 10 - ligne 17 *	1,2,9
A	US 4 823 388 A (MIZUTANI HIROYUKI ET AL) 18 avril 1989 * abrégé * * colonne 4, ligne 54 - colonne 5, ligne 28 *	1,2,9
A	WO 96 13920 A (IBM ;TSUDIK GENE (CH)) 9 mai 1996 * page 18, ligne 4 - page 19, ligne 6 *	1

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

H04L

1

Date d'achèvement de la recherche	Examinateur
14 janvier 1999	Holper, G

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)